Proving Propositions

Wolfgang Schreiner
Research Institute for Symbolic Computation (RISC-Linz)
Johannes Kepler University, Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at
http://www.risc.uni-linz.ac.at/people/schreine

Overview

- Motivation and Preliminaries
- General Strategies
- Decomposing the Goal
- Deriving New Knowledge

Motivation and Preliminaries

Motivation

Definition: a proof is a structured argument that a proposition is true.

- You claim that a formula is a (true) proposition.
  - You believe that it is true.
- You want to convince yourself about this.
  - You want to make sure that it is true.
- You want to convince someone else about this.
  - You want to make a skeptic opponent admit that it is true.

Proving is the art of (scientifically) arguing.

Proof Rules

- Collection of proof rules.
  - Based on the syntactic structure of formulas.
  - Can decide whether application is correct by looking at syntax.
- Inventing a proof.
  - Creative (non-algorithmic) activity.
  - Proof rules provide a mental skeleton and give some guidelines.
  - Ultimately, some insight is required.
- Checking a proof.
  - Mechanical (algorithmic) activity.
  - Proof rules determine the framework.
  - Everyone is able to read and check a proof.

Every scientist and engineer should understand these rules.

Proof Levels

A proof can be given on various levels of detail.

- Lowest level (most details).
  - Very small reasoning steps.
  - Correctness can be checked by computer program.
  - Proofs become very large.
- Higher level (fewer details).
  - Larger reasoning steps.
  - Proof becomes shorter and manageable by humans.
  - Each step can be decomposed into finer steps.

A high-level proof is a map of a (more detailed but larger) low-level proof; it can be refined on demand.

Knowledge

A proof is relative to given knowledge.

- Axioms (characterization of the considered domain),
- Definitions (a "harmless" extension of the domain),
- Tautologies (true propositions in every domain),
- Propositions (formulas that have been previously proved),
- Assumptions (knowledge gradually added in a proof).

Proof Situations

Definition: a proof situation consists of available knowledge K (a set of formulas assumed true) and the goal G (a formula to be proved).

$$\begin{array}{|c|}\hline K \\ \hline G \\ \hline\end{array}$$

"We (have to) prove G with knowledge K."

- The knowledge available in a particular situation is typically not explicitly written down.
- Knowledge at the beginning of the proof extended by all definitions and assumptions in the proof branch that led to the situation.

Proof Rule

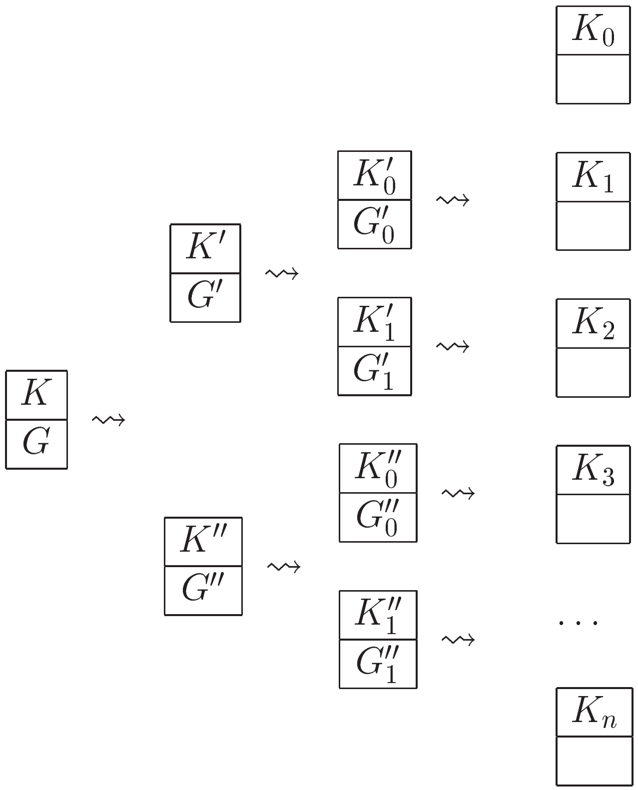
Definition: a proof rule reduces a proof situation to one or more other situations.

$$\begin{array}{|c|}\hline K_0 \\ \hline G_0 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K_1 \\ \hline G_1 \\ \hline \end{array}$$

"In order to prove G_0 with knowledge K_0 it suffices to prove G_1 with knowledge K_1".

Definition: a proof is the reduction of the start situation to other situations that are again reduced to other situations until we have only situations in which nothing is left to be proved.

Proof Tree



Proof Completion

Proposition: For proving with knowledge $K \cup \{G\}$ the goal G, nothing has to be done any more.

$$\boxed{\begin{array}{c} K \cup \{G\} \\ \hline G \end{array}} \leadsto \boxed{\begin{array}{c} K \cup \{G\} \\ \hline \end{array}}$$

The only rule to terminate a proof branch.

General Strategies

General Strategies

- Direct proofs
  - Try to prove the goal.
  - Try to prove the negation of the goal.
- Indirect proofs.
  - Assume the goal does not hold and derive a contradiction.
  - Assume the goal does hold and derive a contradiction.

Two basic approaches in two variants.

Direct Proof

Given some knowledge K and a goal G.

1. We try $\boxed{\frac{K}{G}}$. If we are successful, then G holds.
2. We try $\boxed{\frac{K}{\neg G}}$. If we are successful, then $\neg G$ holds.

We do not know in advance whether G is true!

Contradictions

Proposition: For proving with knowledge K the goal G, it suffices to prove $\mathrm{F(alse)}$ with additional knowledge $\neg G$.

$$\frac{K}{G} \rightsquigarrow \frac{K \cup \{\neg G\}}{\mathrm{F(alse)}}$$

"We assume $\neg G$ and show a contradiction".

Try to derive a contradiction.

Contradiction

A contradiction is usually derived by establishing a proof situation

$$\begin{array}{|c|}\hline K \cup \{G, \neg G\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array}$$

because we then immediately have

$$\begin{array}{|c|}\hline K \cup \{G, \neg G\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \cup \{\mathrm{F(alse)}\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \cup \{\mathrm{F(alse)}\} \\ \hline \\ \hline \end{array}.$$

Try to prove a formula that contradicts some given knowledge.

Example

We show

$$\forall x \in \mathbb{Q} : x * x \neq 2.$$

Take arbitrary $x \in \mathbb{Q}$. We assume (1) $x * x = 2$ and show a contradiction.

From the construction of $\mathbb{Q}$, we know $x = \frac{a}{b}$ for some $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$ such that (2) $\mathrm{N}(a)$ and $\mathrm{N}(b)$ are relatively prime. We have $\frac{a \, *_{\mathbb{Z}} \, a}{b \, *_{\mathbb{Z}} \, b} = 2$ and thus (from now on we operate in $\mathbb{Z}$ and drop the corresponding subscripts):

$$(3)\ a * a = 2 * b * b.$$

From (3) we know $\mathrm{N}(2)|\mathrm{N}(a * a)$ and thus also (4) $\mathrm{N}(2)|\mathrm{N}(a)$ (a proposition that has to be proved extra). Therefore there exists some $c \in \mathbb{Z}$ such that

$$(5)\ a = 2 * c.$$

From (3) and (5) we have $2 * c * 2 * c = 2 * b * b$, i.e., $2 * c * c = b * b$, thus (6) $\mathrm{N}(2)|\mathrm{N}(b * b)$ and therefore (7) $\mathrm{N}(2)|\mathrm{N}(b)$. (4) and (7) contradict (2).

Indirect Proof

Given some knowledge K and a goal G.

1. We try $\boxed{\dfrac{K \cup \{\neg G\}}{\mathrm{F(alse)}}}$. If we are successful, then G holds.
2. We try $\boxed{\dfrac{K \cup \{G\}}{\mathrm{F(alse)}}}$. If we are successful, then $\neg G$ holds.

We will see some examples for special situations.

Proof Directions

1. **Top-Down**: decomposing the goal into simpler formulas with corresponding subproofs.

$$\boxed{\begin{array}{c} K \\ \hline G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K_0 \\ \hline G_0 \end{array}} \ldots \boxed{\begin{array}{c} K_{n-1} \\ \hline G_{n-1} \end{array}}$$

2. **Bottom-Up**: deriving new knowledge from the given knowledge such that the goal ultimately becomes part of the knowledge.

$$\boxed{\begin{array}{c} K \\ \hline G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \cup \{F\} \\ \hline G \end{array}}$$

We usually begin with the top-down strategy.

Decomposing the Goal

Decomposing the Goal

- Decomposition of universally quantified formulas,
- Decomposition of existentially quantified formulas,
- Decomposition of equivalences,
- Decomposition of implications,
- Decomposition of conjunctions,
- Decomposition of disjunctions.
- Inserting predicate and function definitions.

Decompositon determined by outermost quantifier/connective.

Decomposition of Universally Quantified Formulas

Proposition: For proving with knowledge K the goal $\forall x : G$, it suffices to prove $G[x \leftarrow a]$ where a is an object constant that does not appear in K and not in G.

$$\boxed{\begin{array}{c} K \\ \hline \forall x : G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \\ \hline G[x \leftarrow a] \end{array}} \; (a \text{ not in } K \cup \{G\})$$

"We prove $(\forall x : G)$. We take an arbitrary (but fixed) constant a and show $G[x \leftarrow a]$."

No knowledge is available about constant yet.

Typical Constant Names

- Choose a constant name that reflects the name of the variable.

  "We prove $(\forall x : G)$. We take an arbitrary constant x_0 and show $G[x \leftarrow x_0]$."

- Choose the variable name itself as the constant name.

  "We prove $(\forall x : G)$. We take an arbitrary constant x and show G."

  "We prove $(\forall x : G)$. Take arbitrary x. Then ... (proof of G)."

Constant name must not yet appear in knowledge or goal!

Example

We show

$$\forall x \in \mathbb{Z}, y \in \mathbb{Z} : x + y = y + x.$$

Take arbitrary $x_0 \in \mathbb{Z}, y_0 \in \mathbb{Z}$. We have to show

$$x_0 + y_0 = y_0 + x_0.$$

We know

$$\begin{aligned} x_0 + y_0 &= \text{(definition of } +\text{)} \\ \mathrm{I}(x_0 +_{\mathbb{N}} y_0, x_1 +_{\mathbb{N}} y_1) &= \text{(commutativity of } +_{\mathbb{N}}\text{)} \\ \mathrm{I}(y_0 +_{\mathbb{N}} x_0, y_1 +_{\mathbb{N}} x_1) &= \text{(definition of } +\text{)} \\ y_0 + x_0. & \end{aligned}$$

Example

We show

$$\forall x \in \mathbb{Z}, y \in \mathbb{Z} : x + y = y + x.$$

Take arbitrary $x \in \mathbb{Z}, y \in \mathbb{Z}$. We have

$$\begin{aligned} x + y &= (\text{definition of } +) \\ \mathrm{I}(x +_{\mathbb{N}} y, x +_{\mathbb{N}} y) &= (\text{commutativity of } +_{\mathbb{N}}) \\ \mathrm{I}(y +_{\mathbb{N}} x, y +_{\mathbb{N}} x) &= (\text{definition of } +) \\ y + x. \end{aligned}$$

More typical version.

Indirect Method for Universal Formulas

Instead of proving $(\forall x : G)$ we assume $(\neg\forall x : G)$, i.e., $(\exists x : \neg G)$ and proceed to derive a contradiction:

$$\boxed{\begin{array}{c} K \\ \hline \forall x : G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \cup \{\exists x : \neg G\} \\ \hline \mathrm{F(alse)} \end{array}} \quad \left(\rightsquigarrow \boxed{\begin{array}{c} K \cup \{\neg G[x \leftarrow a]\} \\ \hline \mathrm{F(alse)} \end{array}} \right)$$

"We prove $(\forall x : G)$. Assume $\neg G$ for some x. Then ... (derivation of a contradiction with additional knowledge $\neg G$)."

We will see later how to work with existential formulas in knowledge.

Decomposition of Existential Quantifications

Proposition: For proving with knowledge K the goal $\exists x : G$, it suffices to prove $G[x \leftarrow T]$ for some term T.

$$\begin{array}{|c|}\hline K \\ \hline \exists x : G \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \\ \hline G[x \leftarrow T] \\ \hline \end{array}$$

"We have to prove $(\exists x : G)$. We prove $G[x \leftarrow T]$".

We have to find a witness, i.e., a value for x that makes G true.

Typical Use

- Introduce a new constant name

  "We have to prove $(\exists x : G)$. Take $a := T$. We prove $G[x \leftarrow a]$".

- Use the variable name as the constant name

  "We have to prove $(\exists x : G)$. Take $x := T$. We then have ... (proof of G with additional knowledge $x = T$)."

Constant name must not yet appear in knowledge or goal!

Example

Proposition: Between any two rational numbers, there is another rational number:

$$\forall x \in \mathbb{Q}, y \in \mathbb{Q} : x < y \Rightarrow \exists z \in \mathbb{Q} : x < z < y.$$

Proof: Take arbitrary $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$ with $x < y$. Then $x < (x+y)/2 < y$ because ...

Proof: Take arbitrary $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$ with $x < y$. Let $a := (x+y)/2$. Then $x < a < y$ because ...

Proof: Take arbitrary $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$ with $x < y$. Let $z := (x+y)/2$. Then $x < z < y$ because ...

Indirect Method for Existential Formulas

Instead of proving $(\exists x : G)$, we assume $(\neg\exists x : G)$, i.e., $(\forall x : \neg G)$ and deriving a contradiction:

$$\boxed{\begin{array}{c} K \\ \hline \exists x : G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \cup \{\forall x : \neg G\} \\ \hline \mathrm{F(alse)} \end{array}}.$$

"We prove $(\exists x : G)$. Assume $(\forall x : \neg G)$. Then ... (derivation of a contradiction with additional knowledge $(\forall x : \neg G)$)."

We will see later how to work with universal formulas in knowledge.

Decomposition of Equivalences

Proposition: For proving with knowledge K the goal $G_0 \Leftrightarrow G_1$, it suffices to prove both $G_0 \Rightarrow G_1$ and $G_1 \Rightarrow G_0$:

$$\begin{array}{|c|}\hline K \\ \hline G_0 \Leftrightarrow G_1 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \\ \hline G_0 \Rightarrow G_1 \\ \hline \end{array} \begin{array}{|c|}\hline K \\ \hline G_1 \Rightarrow G_0 \\ \hline \end{array}$$

An equivalence is shown by proving the implication "from left to right" and "from right to left"

Typical Use

We prove $G_0 \Leftrightarrow G_1$:

- $\Rightarrow$: ... (proof of $G_0 \Rightarrow G_1$).
- $\Leftarrow$: ... (proof of $G_1 \Rightarrow G_0$).

We prove $G_0 \Leftrightarrow G_1 \Leftrightarrow G_2$, i.e., $(G_0 \Leftrightarrow G_1) \wedge (G_1 \Leftrightarrow G_2)$:

- $G_0 \Rightarrow G_1$,
- $G_1 \Rightarrow G_2$,
- $G_2 \Rightarrow G_0$.

Traverse the "implication circle"!

Example

Proposition: For every x and y, we have

$$x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x).$$

Proof: Take arbitrary x and y. We prove $x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x)$.

- We prove $x = y \Rightarrow (x \subseteq y \wedge y \subseteq x)$. ...
- We prove $(x \subseteq y \wedge y \subseteq x) \Rightarrow x = y$. ...

Decomposition of Implications

For proving with knowledge K the goal $G_0 \Rightarrow G_1$, it suffices to prove G_1 with additional knowledge G_0:

$$\boxed{\begin{array}{c} K \\ \hline G_0 \Rightarrow G_1 \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \cup \{G_0\} \\ \hline G_1 \end{array}}$$

"We show $G_0 \Rightarrow G_1$. Assume G_0. Then ... (proof of G_1 with additional knowledge G_0)."

Add the hypothesis to the knowledge and prove the conclusion.

Example

Proposition: For every x and y, we have

$$x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x).$$

Proof: Take arbitrary x and y. We prove $x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x)$.

- We prove $x = y \Rightarrow (x \subseteq y \wedge y \subseteq x)$. Assume $x = y$, i.e., by definition of '$=$',

  $$(1)\ \forall z : z \in x \Leftrightarrow z \in y.$$

  We prove $x \subseteq y \wedge y \subseteq x$. ...
- ...

Alternative

Because of $(G_0 \Rightarrow G_1)$ iff $(\neg G_1 \Rightarrow \neg G_0)$, it suffices to prove

$$\begin{array}{|c|}\hline K \\ \hline G_0 \Rightarrow G_1 \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{|c|}\hline K \cup \{\neg G_1\} \\ \hline \neg G_0 \\ \hline \end{array}$$

"We show $G_0 \Rightarrow G_1$. Assume $\neg G_1$. Then ... (proof of $\neg G_0$ with additional knowledge $\neg G_1$)."

Reverse the direction of the implication.

Indirect Method for Implications

Because of $\neg(G_0 \Rightarrow G_1)$ iff $(G_0 \wedge \neg G_1)$, it suffices to prove

$$\frac{K}{G_0 \Rightarrow G_1} \quad \rightsquigarrow \quad \frac{K \cup \{G_0 \wedge \neg G_1\}}{\mathrm{F(alse)}}$$

"We have to show $G_0 \Rightarrow G_1$. Assume $G_0 \wedge \neg G_1$. Then we have ... (derivation of a contradiction)".

Add the hypothesis and the negation of the conclusion to the knowledge and derive a contradiction.

Decomposition of Conjunctions

Proposition: For proving with knowledge K the goal $G_0 \wedge G_1$, it suffices to prove both G_0 and G_1:

$$\begin{array}{|c|}\hline K \\ \hline G_0 \wedge G_1 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \\ \hline G_0 \\ \hline \end{array} \begin{array}{|c|}\hline K \\ \hline G_1 \\ \hline \end{array}$$

We have to show $G_0 \wedge G_1$.

1. ... (proof of G_0).
2. ... (proof of G_1).

A conjunction is shown by showing both conjuncts in turn.

Example

Proposition: For every x and y, we have

$$x = y \Leftrightarrow (x \subseteq y \land y \subseteq x).$$

Proof: Take arbitrary x and y. We prove $x = y \Leftrightarrow (x \subseteq y \land y \subseteq x)$.

- We prove $x = y \Rightarrow (x \subseteq y \land y \subseteq x)$. Assume $x = y$. We have to prove $x \subseteq y \land y \subseteq x$.
  - We prove $x \subseteq y$. ...
  - We prove $y \subseteq x$. ...
- ...

Indirect Method for Conjunctions

Because of $\neg(G_0 \wedge G_1)$ iff $\neg G_0 \vee \neg G_1$, the indirect method leads to

$$\begin{array}{|c|}\hline K \\ \hline G_0 \wedge G_1 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \cup \{\neg G_0 \vee \neg G_1\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \cup \{\neg G_0\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array} \begin{array}{|c|}\hline K \cup \{\neg G_1\} \\ \hline \mathrm{F(alse)} \\ \hline \end{array}$$

We have to prove $G_0 \wedge G_1$.

- Assume $\neg G_0$. Then ... (derivation of a contradiction.)
- Assume $\neg G_1$. Then ... (derivation of a contradiction.)

We will see later this technique of "case distinction".

Decomposition of Disjunctions

Proposition: For proving with knowledge K the goal $G_0 \vee G_1$, it suffices to prove G_1 with additional knowledge $\neg G_0$:

$$\frac{K}{G_0 \vee G_1} \rightsquigarrow \frac{K \cup \{\neg G_0\}}{G_1}$$

"We have to show $G_0 \vee G_1$. Assume $\neg G_0$. Then ... (proof of G_1)."

- Consequence of "$(G_0 \vee G_1)$ iff $(\neg G_0 \Rightarrow G_1)$".
- Roles of G_0 and G_1 can be inverted.

Same techniques as for decomposition of implications.

Explicitly Defined Predicates

Proposition: For proving an atomic formula $p(a_0, \ldots, a_{n-1})$ with

$$p(x_0, \ldots, x_{n-1}) :\Leftrightarrow G,$$

it suffices to prove $G[x_0 \leftarrow a_0, \ldots, x_{n-1} \leftarrow a_{n-1}]$:

$$\frac{K \cup \{\forall x_0, \ldots, x_{n-1} : p(x_0, \ldots, x_{n-1}) \Leftrightarrow G\}}{p(a_0, \ldots, a_{n-1})} \rightsquigarrow$$

$$\frac{K \cup \{\forall x_0, \ldots, x_{n-1} : p(x_0, \ldots, x_{n-1}) \Leftrightarrow G\}}{G[x_0 \leftarrow a_0, \ldots, x_{n-1} \leftarrow a_{n-1}]}$$

Insert the definition of the predicate!

Example

Proposition: For every x and y, we have

$$x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x).$$

Proof: Take arbitrary x and y. We prove $x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x)$.

- We prove $x = y \Rightarrow (x \subseteq y \wedge y \subseteq x)$. Assume $x = y$. We have to prove $x \subseteq y \wedge y \subseteq x$.
  - We prove $x \subseteq y$, i.e., by definition of '$\subseteq$', $\forall z \in x : z \in y$. ...
  - ...
- ...

Explicitly Defined Functions

Proposition: For proving the goal $G[x \leftarrow F(a_0, \ldots, a_{n-1})]$ with

$$F(x_0, \ldots, x_{n-1}) := T,$$

it suffices to prove $G[x \leftarrow T[x_0 \leftarrow a_0, \ldots, x_{n-1} \leftarrow a_{n-1}]]$:

$$\frac{K \cup \{\forall x_0, \ldots, x_{n-1} : F(x_0, \ldots, x_{n-1}) = T\}}{G[x \leftarrow F(a_0, \ldots, a_{n-1})]} \rightsquigarrow$$

$$\frac{K \cup \{\forall x_0, \ldots, x_{n-1} : F(x_0, \ldots, x_{n-1}) = T\}}{G[x \leftarrow T[x_0 \leftarrow a_0, \ldots, x_{n-1} \leftarrow a_{n-1}]]}$$

Insert the definition of the function!

Example

We prove

$$\forall x : x' \neq 0.$$

Take arbitrary x. By definition of 0 and $'$, it suffices to prove

$$x \cup \{x\} \neq \emptyset$$

which is true because $x \in (x \cup \{x\})$ but $x \neq \emptyset$.

Deriving New Knowledge

Proof by Case Distinction

Proposition: For proving with knowledge K the goal G, it suffices to prove G with additional knowledge F and to prove G with additional knowledge $\neg F$ (for some formula F).

$$\begin{array}{|c|}\hline K \\ \hline G \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{|c|}\hline K \cup \{F\} \\ \hline G \\ \hline \end{array} \begin{array}{|c|}\hline K \cup \{\neg F\} \\ \hline G \\ \hline \end{array}$$

We have to prove G.

1. Assume F. Then ... (proof of G with additional knowledge F).
2. Assume $\neg F$. Then ... (proof of G with additional knowledge $\neg F$).

Decompose the universe of situations by an assumption.

Example

We prove $\forall x \in \mathbb{R} : x * x \neq -1$. Take arbitrary $x \in \mathbb{R}$.

- If $x \geq 0$, then $x * x \geq 0$.
- If $x < 0$, then also $x * x \geq 0$.

Typical Use

We have a formula $(F_0 \vee \ldots \vee \ldots F_{n-1})$ in our knowledge:

$$\boxed{\begin{array}{c} K \cup \{F_0 \vee \ldots \vee F_{n-1}\} \\ \hline G \end{array}} \quad \rightsquigarrow \quad \boxed{\begin{array}{c} K \cup \{F_0\} \\ \hline G \end{array}} \quad \ldots \quad \boxed{\begin{array}{c} K \cup \{F_{n-1}\} \\ \hline G \end{array}}$$

We have to prove G. Since we know $(F_0 \vee \ldots \vee F_{n-1})$, it suffices to consider the following cases:

- Case F_0: $\ldots$ (proof of G with additional knowledge F_0).
- $\ldots$
- Case F_{n-1}: $\ldots$ (proof of G with additional knowledge F_{n-1}).

Universal Quantification in Knowledge

Proposition: For proving with knowledge $K \cup \{\forall x : F\}$ the goal G, it suffices to prove G with additional knowledge $F[x \leftarrow T]$ for any term T:

$$\begin{array}{|c|}\hline K \cup \{\forall x : F\} \\ \hline G \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{|c|}\hline K \cup \{\forall x : F, F[x \leftarrow T]\} \\ \hline G \\ \hline \end{array}$$

"We have to prove G. Since we know $(\forall x : F)$, we have $F[x \leftarrow T]$ and thus ... (proof of G with additional knowledge $F[x \leftarrow T]$)."

A formula $(\forall x : F)$ in the knowledge is a machine that takes any T and produces additional knowledge $F[x \leftarrow T]$.

Example

Proposition: For every x and y, we have

$$x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x).$$

Proof: Take arbitrary x and y. We prove $x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x)$.

- We prove $x = y \Rightarrow (x \subseteq y \wedge y \subseteq x)$. Assume $x = y$, i.e.,

  $$(1)\ \forall z : z \in x \Leftrightarrow z \in y.$$

  We have to prove $x \subseteq y \wedge y \subseteq x$.

  – We prove $x \subseteq y$, i.e., by definition of '$\subseteq$', $\forall w \in x : w \in y$. Take arbitrary w. We have to prove $w \in x \Rightarrow w \in y$. Assume (2) $w \in x$. We have to prove $w \in y$ which is a consequence of (1) (which gives us $w \in x \Leftrightarrow w \in y$) and (2).

  – ...

Existential Quantification in Knowledge

Proposition: For proving with knowledge $K \cup \{\exists x : F\}$ the goal G, it suffices to prove G with additional knowledge $F[x \leftarrow a]$ for some object constant a that does not appear in K, G, or F:

$$\boxed{\begin{array}{c} K \cup \{\exists x : F\} \\ \hline G \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \cup \{\exists x : F, F[x \leftarrow a]\} \\ \hline G \end{array}} \quad (a \text{ not in } K, G, F)$$

“We prove G. Since we know $(\exists x : F)$, we have have some a with $F[x \leftarrow a]$. Thus ... (proof of G with new knowledge $F[x \leftarrow a]$).”

A formula $(\exists x : F)$ in the knowledge base is an “engine” which returns a new constant a about which we know (only) $F[x \leftarrow a]$.

Example

Take arbitrary A, B, C, $f : A \xrightarrow{\text{partial}} B$, and $g : B \to C$. We prove (1) $(f \circ g) : A \xrightarrow{\text{partial}} C$. i.e., by definition of $\xrightarrow{\text{partial}}$, that

$$(3)\ (f \circ g) \subseteq A \times C;$$
$$(4)\ \forall x, y_0, y_1 : (\langle x, y_0\rangle \in (f \circ g)\ \wedge \langle x, y_1\rangle \in (f \circ g)) \Rightarrow y_0 = y_1.$$

We know (3) from the definition of $\circ$; we still have to show (4). Take arbitrary x, y_0, y_1 and assume

$$(5)\ \langle x, y_0\rangle \in (f \circ g);$$
$$(6)\ \langle x, y_1\rangle \in (f \circ g).$$

We have to show $y_0 = y_1$.
From (5), (6), and the definition of $\circ$, we know $y_0 \in C$, $y_1 \in C$, and

$$(7)\ \exists b \in B : \langle x, b\rangle \in f \wedge \langle b, y_0\rangle \in g;$$
$$(8)\ \exists b \in B : \langle x, b\rangle \in f \wedge \langle b, y_1\rangle \in g.$$

By (7), we have some $b_0 \in B$ such that $\langle x, b_0\rangle \in f \wedge \langle b_0, y_0\rangle \in g$; by (8), we have some $b_1 \in B$ such that $\langle x, b_1\rangle \in f \wedge \langle b_1, y_0\rangle \in g$. ...

Additional Knowledge

Proposition: For proving with knowledge K the goal G, it suffices to prove G with additional knowledge F, if F holds in every domain in which (some of) the formulas in K holds.

$$\begin{array}{|c|}\hline K \\ \hline G \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|}\hline K \cup \{F\} \\ \hline G \\ \hline \end{array} \text{ (}F\text{ holds in every domain in which }K\text{ holds).}$$

Derive new knowledge F from (a subset of) K.

Infering Additional Knowledge

This rule is a "placeholder" for a number of ways to infer $\boxed{\frac{K}{F}}$:

1. This has been shown in a previous proof or is shown as a subproof.
2. This holds because F is a propositional consequence of K, i.e., the conclusion holds independently of the truth values of the atomic formulas and quantified formulas contained in K and F.
3. This is an instance of some quantifier consequence wich give true conclusions in every domain.
4. This is derived by applying substitution rules from known equalities and equivalences.

Propositional Consequences

The following conclusions are propositional consequences for every formula A and B:

Negation

$$\frac{\neg\neg A}{A} \qquad \frac{A}{\neg\neg A}$$

And Introduction and Or Elimination

$$\frac{A \wedge B}{A} \qquad \frac{A}{A \vee B}$$

Propositional Consequences (Continued)

De Morgan

$$\frac{\neg(A \land B)}{\neg A \lor \neg B} \qquad \frac{\neg(A \lor B)}{\neg A \land \neg B} \qquad \frac{\neg A \lor \neg B}{\neg(A \land B)} \qquad \frac{\neg A \land \neg B}{\neg(A \lor B)}$$

Modus Ponens

$$\frac{A, A \Rightarrow B}{B}$$

Contraposition

$$\frac{A \Rightarrow B}{\neg B \Rightarrow \neg A} \qquad \frac{\neg A \Rightarrow \neg B}{B \Rightarrow A} \qquad \frac{A \Leftrightarrow B}{\neg A \Leftrightarrow \neg B} \qquad \frac{\neg A \Leftrightarrow \neg B}{A \Leftrightarrow B}$$

Tautologies

Definition: A propositional formula with variables as subformulas is a (propositional) tautology if it is true for every assignment of truth values to the variables.

Example: $A \lor \neg A$ is a tautology.

Consequence: A general strategy to show that $\boxed{\frac{A}{B}}$ is a propositional consequence is to show that $A \Rightarrow B$ is a propositional tautology.

Example

We show that the following is a tautology:

$$((A \lor B) \land (A \Rightarrow C) \land (B \Rightarrow C)) \Rightarrow C.$$

We assume that its truth value is false and then derive a contradiction:

$$\overset{\text{false}}{\overline{\overset{\text{true}}{\overline{\overset{\text{true}}{\overline{((A \lor B)}} \land (\overset{\text{true}}{\overline{\overset{\text{false}}{\overline{A}} \Rightarrow \overset{\text{false}}{\overline{C}}}}) \land (\overset{\text{true}}{\overline{\overset{\text{false}}{\overline{B}} \Rightarrow \overset{\text{false}}{\overline{C}}}}))}} \Rightarrow \overset{\text{false}}{\overline{C}}}}$$

Because the implication is false, C is false and the conjuncts are true. Thus A and B must be false. Therefore $A \lor B$ is false, which contradicts above derivation.

Quantifier Consequences

For every formula A and B, the following conclusions hold:

Universal Quantification and Conjunction

$$\frac{(\forall x : A \land B)}{(\forall x : A) \land (\forall x : B)} \qquad \frac{(\forall x : A) \land (\forall x : B)}{(\forall x : A \land B)}$$

Existential Quantification and Disjunction

$$\frac{(\exists x : A \lor B)}{(\exists x : A) \lor (\exists x : B)} \qquad \frac{(\exists x : A) \lor (\exists x : B)}{(\exists x : A \lor B)}$$

Quantifier Consequences (Continued)

Universal and Disjunction, Existential and Conjunction

$$\frac{(\forall x : A) \lor (\forall x : B)}{(\forall x : A \lor B)} \qquad \frac{(\exists x : A \land B)}{(\exists x : A) \land (\exists x : B)}$$

Universal and Existential Quantification

$$\frac{\exists x : \forall y : A}{\forall y : \exists x : A}$$

Quantifier Consequences (Continued)

De Morgan Laws

$$\frac{\neg\forall x : A}{\exists x : \neg A} \qquad \frac{\exists x : \neg A}{\neg\forall x : A} \qquad \frac{\neg\exists x : A}{\forall x : \neg A} \qquad \frac{\forall x : \neg A}{\neg\exists x : A}$$

Such Quantifier

$$\frac{\exists x : A}{A[x \leftarrow \textbf{such } x : A]}$$

$$\frac{(\forall y_0, y_1 : (A[x \leftarrow y_0] \wedge A[x \leftarrow y_1]) \Rightarrow y_0 = y_1)}{(\forall x : A \Rightarrow x = \textbf{such } x : A)}$$

Example

We show for arbitrary formula A

$$(\neg\forall x : A) \Rightarrow (\exists x : \neg A)$$

by showing (contraposition)

$$(\neg\exists x : \neg A) \Rightarrow (\neg\neg\forall x : A)$$

i.e. (propositional consequence and substitution, see next subsection)

$$(\neg\exists x : \neg A) \Rightarrow (\forall x : A).$$

We assume $(*)$ $\neg\exists x : \neg A$ and show $\forall x : A$. Take arbitrary and assume $\neg A$. Then we have $(\exists x : \neg A)$ which contradicts (*).

Substitutions

For all terms S and T, formulas A and B, variables x and formula patterns C with variable F, the following holds:

Equality Subsitutions

$$\frac{S = T \wedge A[x \leftarrow S]}{A[x \leftarrow T]}$$

Equivalence Substitutions

$$\frac{A \Leftrightarrow B \wedge C[F \leftarrow A]}{C[F \leftarrow B]}$$

Replace "equal things by equal things", e.g., insert definitions.

Summary

- Proving versus disproving.
- Direct method versus indirect method.
- Top-down decomposition.
  - Outermost quantifier/connective.
  - Inserting definitions.
- Deriving new knowledge.
  - Case distinctions.
  - Application of universally/existentially formulas in knowledge.
  - Propositional tautologies.
  - Quantifier consequences.
  - Substitutions.